

**UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA**

IN THE MATTER OF THE SEARCH OF:
DROPBOX, INC.
185 BERRY STREET, 4TH FLOOR
SAN FRANCISCO, CALIFORNIA 94107

Magistrate No. 17-1156
[UNDER SEAL]

Dropbox.com accounts associated with the
following email addresses and attached
URLs:

Woodsfamilyhome@gmail.com

Chris@ustechsolutions.com

cwoods@teksystems.com

bigmaninpa@gmail.com

bigmaninpa16@gmail.com

Chriswoods72@outlook.com

Chriswoods@synergy.com

Chris.woods@synergy.com

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Thomas Carter, being duly sworn, do hereby depose and state:

I. Introduction

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) assigned to the Pittsburgh, field office. I am currently assigned to the Crimes Against Children Task Force (CACTF). I have been so employed for approximately 26 years. As a member of the CACTF I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252(a)(2), and 2252(a)(4)(B). I have had the

opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also participated in the execution of numerous search warrants, many of which involved child exploitation and/or child pornography offenses.

II. Purpose of the Affidavit

2. This affidavit is made in support of a search warrant for information associated with URLs listed in Attachment A and incorporated herein and/or the following accounts:

Woodsfamilyhome@gmail.com

Chris@ustechsolutions.com

cwoods@teksystems.com

bigmaninpa@gmail.com

bigmaninpa16@gmail.com

Chriswoods72@outlook.com

Chriswoods@synergy.com

Chris.woods@synergy.com

that are stored at a premises owned, maintained, controlled, or operated by Dropbox, Inc., a file syncing and collaboration service that allows users to access and share their files on computers, phones, tablets, and the Dropbox website headquartered at 185 Berry Street, 4th Floor, San Francisco, California 94107. The information to be searched is described in the following paragraphs and in Attachment A, which is attached hereto and made a part hereof. This affidavit is made in support of an application for a search warrant under Title 18, United States Code, Sections 2252(a)(2) and (a)(4), involving the use of a computer and/or cellular telephone in or affecting interstate commerce to transport, advertise, receive, distribute, possess and/or access

child pornography; to require Dropbox, Inc., to disclose to the government records and other information in its possession pertaining to the customer(s) associated with the aforementioned email accounts and/or URLs more particularly described in Attachment A.

3. Your Affiant is requesting authority to search the accounts where the items specified in Attachment A may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crimes.

4. Because the purpose of this affidavit is to set forth only the facts necessary to establish probable cause for a search warrant for the pertinent account, I have not described all the facts and circumstances of which I am aware. I have set forth only the facts I believe necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252(a)(2) and 2252(a)(4)(B), involving the use of a computer and/or cellular telephone in or affecting interstate commerce to access, possess, distribute or receive child pornography, are presently located within the accounts associated with the aforementioned email addresses.

5. Facts not set forth herein are not relied upon in support of my conclusion that probable cause exists. Where statements of others are set forth in this affidavit, they are set forth in substance and in part. The information contained in this affidavit is based upon my personal knowledge and observation, my training and experience, conversations with other law enforcement officers and witnesses, and the review of documents and records.

6. This affidavit is submitted in support of an application for a search warrant authorizing the search and seizure of Dropbox.com (hereinafter referred to as Dropbox) accounts associated with the below listed email addresses that were/are used by CHRISTOPHER WOODS,

white male DOB: 05/09/1972, previous cellular phone: 724-777-2703, current cellular telephone; 724-553-0009, work phone, 412-904-5300, presently employed by the Synergy placement agency:

Woodsfamilyhome@gmail.com

Chris@ustechsolutions.com

cwoods@teksystems.com

bigmaninpa@gmail.com

bigmaninpa16@gmail.com

Chriswoods72@outlook.com

Chriswoods@synergy.com

Chris.woods@synergy.com

This affidavit is also submitted in support of the search for and seizure of any images that are or were associated with specific Dropbox, Inc., URL addresses, known to have been accessed by WOODS and itemized in Attachment A.

The purpose of this application is to seize evidence, contraband, fruits, and other items related to violations of 18 U.S.C. § 2252(a)(2), which criminalizes the receipt and distribution of child pornography in interstate commerce by computer, and violations of 18 U.S.C. § 2252(a)(4)(B), which criminalizes the possession or access with intent to view child pornography (collectively, the "Specified Federal Offenses").

7. As more described more fully below, there is probable cause to believe that there is evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252(a)(2) and (a)(4)(B), located in the Dropbox.com accounts associated with the aforementioned email accounts and/or associated with the URL's listed in Attachment A.

III. Legal Authority

8. The legal authority for this search warrant application is derived from Title 18, United States Code, Chapter 121, § 2701-11, entitled, “stored wire and electronic communications and transactional records access.”

9. 18 U.S.C. § 2703(c)(A) allows for nationwide service of process of search warrants for the contents of electronic communications. Pursuant to 18 U.S.C. § 2703, as amended by the USA Patriot Act, Section 220, a government entity may require a provider of an electronic communication service or a remote computing service to disclose a record or other information pertaining to a subscriber or customer of such service pursuant to a warrant issued using procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation.

10. This Court has jurisdiction to issue the requested warrants because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, the Court is “a district court of the United States (including a magistrate judge of such a court) .. that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). This Court has jurisdiction over the offense under investigation because the aforementioned email accounts have been used in the Western District of Pennsylvania for communications and because the sexually explicit images recovered from WOODS storage media were accessed, possessed and received in the Western District of Pennsylvania.

11. 18 U.S.C. § 2703 further states in part:

(a) Contents of Wire or Electronic Communications in Electronic Storage. – A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that

is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communication system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of Wire or Electronic Communications in a Remote Computing Service. - (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2)¹ of this subsection -

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant ..

12. 18 U.S.C. § 2703(c)(2) adds that a provider of an electronic communication service or remote computer service must also provide, without notice to the customer, the name, address, connection records, length of service, and means of payment pursuant to a search warrant.

¹ Paragraph (2) of 18 U.S.C. § 2703 states, "[p]aragraph 1 is applicable with respect to any wire or electronic communication that is held or maintained on that service-

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing."

13. 18 U.S.C. § 2252(a)(2) prohibits a person from knowingly receiving or distributing any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contained materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involved the use of a minor engaging in sexually explicit conduct and the visual depiction is of such conduct.

14. 18 U.S.C. § 2252(a)(4)(B) prohibits a person from knowingly possessing, or knowingly accessing with intent to view any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the producing of such visual depiction involved the use of a minor engaging in sexually explicit conduct and the visual depiction is of such conduct.

IV. Definitions

15. The following definitions apply to this Affidavit:

a. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been

created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)).

c. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

d. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

e. “Computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” Cellular telephones often function as computers pursuant to this definition.

f. “Minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

g. “Internet Service Providers” (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or

satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an “email address,” an email mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password. ISPs maintain records (“ISP records”) pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), email communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long term storage of electronic communications and many other types of electronic data and files. Typically, email that has not been opened by an ISP customer is stored temporarily by an ISP incident to the transmission of that email to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is defined by statute as “electronic storage,” see 18 U.S.C. § 2510(17), and the provider of such a service is an “electronic communications service.”

h. An “electronic communications service,” as defined by statute, is “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15). A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by

the recipient, or provides other long term storage services to the public for electronic data and files, is defined by statute as providing a “remote computing service.” 18 U.S.C. § 2711(2).

i. “Domain names” are common, easy to remember names associated with an Internet Protocol address. For example, a domain name of “www.usdoj.gov” refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top-level domains, are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and, .edu for educational organizations. Second level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

j. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet.

V. Facts Establishing Probable Cause

16. Christopher WOODS was married to Jennifer Lynn Woods and the couple had two children. During the time relevant to the crimes described, WOODS and the family lived at 202 North Jackson Street, Evans City, PA, 16033. From January 3-7, 2015, Jennifer Woods discovered emails and images on a computer in her home used exclusively by her husband that were sexually

explicit and appeared to depict children engaged in sexually explicit conduct. Ms. Woods also discovered communications in which her husband discussed buying, selling, and trading images of children who appeared to be under the age of 18.

17. Ms. Woods reported the content she discovered on the computer to the local police. Ms. Woods went to the Evans City Police department and the Butler County District Attorney's office. Ms. Woods provided a written statement in which she described finding two email accounts with over 40,000 emails spanning eight years. Ms. Woods observed nude photographs of girls that appeared to be prepubescent and some sexually explicit communications between her husband and girls claiming to be 13-15 years old and some younger. According to Ms. Woods, in the communications, her husband also shared non-sexual pictures of Ms. Woods and their teenage daughter that had been placed on Facebook, but engaged in sexual chat about the two of them with others. Also in the communications, Christopher WOODS admitted to masturbating into his daughter's underwear and expressed a desire to masturbate and ejaculate onto her breasts. Ms. Woods downloaded some of these chats, images and emails onto a portable "thumb-drive" and subsequently took the thumb-drive to the Evans City Police. On January 8, 2015, the Evans City Police briefly accessed the thumb-drive provided by Ms. Woods and applied for a local search warrant for the residence of the WOODS family located at 202 North Jackson Street, Evans City, Pennsylvania 16033. The search was executed on the same day and a number of items were seized by the Evans City/Seven Fields Regional Police.

18. On April 27, 2017, your Affiant met with patrolman Scott M. Longdon of the Evans City/Seven Fields Regional Police at the Butler County District Attorney's office. Officer Longdon affirmed the circumstances that preceded the execution of the search warrant at the Wood's residence in 2015. He also verified that the electronic devices that were seized in this

investigation had been maintained in the custody of law enforcement continually since their seizure on January 8, 2015.

19. On May 3, 2017, your Affiant interviewed Jennifer Woods at the Pittsburgh FBI Office regarding her observations in 2015. Ms. Woods also clarified that one of the email accounts used by Christopher WOODS that engaged in the sexual communications with others was bigmaninpa@gmail.com. Ms. Woods verified the information she previously provided to law enforcement. Mr. and Mrs. Woods are now divorced. According to Ms. Woods, she has known Christopher WOODS to utilize additional emails for his communications, other than bigmaninpa@gmail.com, including chris@ustechsolutions.com. The computer that contained the sexual images and content that was discovered by Ms. Woods was characterized as Christopher WOODS “work” laptop.

20. On May 10, 2017, the Evans City police tendered custody of computers and storage media obtained in the course of the investigation of Christopher WOODS to the FBI to allow for federal investigation and further forensic analysis. All of the evidence is currently maintained at the Pittsburgh office of the FBI. Federal warrants for the examination of the computers and storage media seized from Christopher WOODS were obtained from this Court (Magistrate Judge Lenihan) on May 24, 2017.

21. Your Affiant has reviewed the gray Lexar Thumb-drive originally obtained by the Evans City Police department from Jennifer Woods. My review of the content of this thumb-drive revealed an email conversation between “cobra Dragon” using email of Alittlegirlie@yahoo.com and Bigmaninpa@gmail.com. (Bigmaninpa@gmail.com was the email address Christopher Woods used in January 2015). Among the contents on the thumb drive, “Cobra Dragon” forwarded an email from his email address Alittlegirlie@yahoo.com from guycyryus@yahoo.com

which contained 5 images of young girls approximately 10-12 years old. Four images depict the young girls in swimwear and/or underwear. One image depicts a pre-pubescent girl who appears to be 10-12 years old and nude. The child is positioned on all fours and her genitals are exposed from the rear.

22. The corresponding email discussion focuses upon the sexually explicit image of the nude image of the female child. As bigmaninpa@gmail.com WOODS comments, “They last one is a nice view Does tgat look like you. Are you as young and tiny as the cutie in the bikini?” “Cobra Dragon/Alittlegirlie@yahoo.com replies, “lol im a little older than that but not much.”

23. Records indicate Christopher WOODS presently resides in Cranberry Township, Pennsylvania. Records further indicate a mailing address of P.O. Box 1562, Creekview Circle, Apartment 1401, Cranberry Township, Pennsylvania, 16066. A review of social media sites as recently as June 2017 revealed that the moniker BigmaninPA still appears to be used by Christopher Woods, according to his image and demographics.

24. On May 24, 2017, your Affiant also obtained a federal search warrant from this Court (Magistrate Judge Lenihan) to search the Facebook account that Jennifer Woods and Christopher WOODS shared during their marriage—set up as “ChrisnJyn.” In 2015, at or about the time that Ms. Woods discovered the sexually explicit chats and images on WOODS’ computer, she also observed sexually explicit messages between Christopher WOODS and others on the Facebook account to which they both had access. Ms. Woods told your Affiant that WOODS would share Facebook images of her, their teenage daughter and their teenage daughters’ friends that were not sexual in nature, but that, in conjunction with sending the images, WOODS would engage in sexually explicit messaging with others about their daughter and their daughter’s friends. He referred to having collected underwear from Jennifer Woods, their daughter and their

daughter's friends and talked about providing it to others. WOODS made other statements indicative of a sexual interest in their daughter. Jennifer Woods informed your Affiant that she had accessed the Facebook page as recently as November 2016 and observed that some of the historical sexual messages were still present on the Facebook account. Following their divorce and separation, Christopher WOODS modified the Facebook page to reflect that it is his personal account and not a joint account. According to Jennifer Woods, however, the account password remained the same and she was able to view the account as recently as May 2017.² In reviewing the records received from Facebook pursuant to the May 24, 2017 federal search warrant, your Affiant found that WOODS is associated with two additional email addresses: woodsfamilyhome@gmail.com and Chris@ustechsolutions.com.

25. On July 20, 2017, your Affiant interviewed the two biological children of Jennifer and Christopher WOODS, now ages seventeen and nineteen. Neither child disclosed sexual contact with WOODS. However, WOODS' daughter, now seventeen years old, told your Affiant about a touching that she did not think was inappropriate at the time but now suspects may have been. His daughter stated that when she was twelve years old and lying with WOODS on the couch to watch television, she remembers her father moving his hand up toward her breast. She also recalled a time that made her uncomfortable--when she was thirteen years old and using her father's cell phone—she discovered pictures of adult women in bikinis. Although it upset her at the time, WOODS' daughter did not know what to do, and she did not tell anyone. Jennifer and Christopher WOODS' son, now nineteen years old, told your Affiant that he and his father were never really close and, after it came out at school that his dad was being investigated for child

² At the time the federal search warrant was approved (May 24, 2017), Jennifer Woods reported that she could not access the Facebook account and told law enforcement that she believed that Christopher WOODS very recently changed the access password.

pornography, he found it odd when some of his classmates told him that his father had been following them on social media sites such as Facebook and Instagram. Cole also informed your Affiant that his father's name on the social media site Snapchat is "Bigmaninpa." Cole knew his father was/is associated with the following email addresses:

woodsfamilyhome@gmail.com (current)

Chriswoods72@outlook.com

Chris.woods@synergy.com (work)

26. Forensic analysis has been and is being conducted upon the cell phone and storage media seized from Christopher WOODS in 2015. Social media chat sessions from Christopher WOODS' cellular telephone include communications and exchange of multiple images of child pornography. In addition, numerous chat sessions using "KIK and "Tumblr" were recovered from the cellular phone that involve WOODS engaging in sexually explicit chats with several individuals.

27. Forensic extraction from WOODS' cellular telephone revealed a list of Dropbox files with the actual URLs associated with each Drop Box entry. Apparent from WOODS' browsing history on his cellular telephone are multiple pages of URLs from Dropbox account locations indicating that WOODS accessed these images. These URLs are associated with titles, some of which suggest sexual content, such as "Dropbox-bondage," "Dropbox-kids," "Dropbox-YoungKikPix," "Dropbox-All My Stuff" and "Dropbox-big red." These files are stored in the accompanying URLs associated with the designated Dropbox account. At present, your Affiant is unable to access these URLs and the associated Dropbox files/folder access to the individual Dropbox account(s).

28. For all of the foregoing reasons, there is probable cause that the Dropbox URLs found in the web browsing history on WOODS' cell phone contain images and/or videos depicting the sexual exploitation of minors. Further, evidence pertaining to the images/videos of child pornography may also be found in the Dropbox account(s) associated with one or more of the following email addresses:

Woodsfamilyhome@gmail.com

Chris@ustechsolutions.com

cwoods@teksystems.com

bigmaninpa@gmail.com

bigmaninpa16@gmail.com

Chriswoods72@outlook.com

Chriswoods@synergy.com

Chris.woods@synergy.com

V. Information That May Be Available From Dropbox, Inc.

29. Dropbox is a file hosting service operated by Dropbox, Inc., headquartered in San Francisco, California, that offers cloud storage, file synchronization, personal cloud, and client software. In my training and experience, I have learned that Dropbox, Inc., provides a variety of on-line services, including on-line storage access to the general public. Dropbox, Inc., allows subscribers to obtain accounts at the domain name www.dropbox.com. Subscribers obtain a Dropbox, Inc., account by registering with an email address. During the registration process, Dropbox, Inc., asks subscribers to provide basic personal information. This information can include the subscriber's full name, physical address, email address, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account

number). Therefore, the computers of Dropbox, Inc., are likely to contain stored electronic communications and files, and information concerning subscribers and their use of Dropbox, Inc. services, such as account access information, file sharing information, and account application information.

30. When a subscriber transfers a file to a Dropbox, Inc. account, it is initiated at the user's computer, phone, tablet, etc., transferred via the Internet to Dropbox, Inc.'s servers, and then can automatically be synchronized and transmitted to other computers or electronic devices that have been registered with that Dropbox, Inc. account. This includes on-line storage in Dropbox, Inc.'s servers. This means that the files and folders created and synchronized in a Dropbox account can then be accessed and viewed, with the same contents, on any electronic device accessing the Dropbox website or application, including the Dropbox mobile phone application. Users can access Dropbox from anywhere in the world using the Internet. For example, a user may take a photograph from a smartphone, upload that photo to Dropbox, and then erase the photo from the user's phone. The photograph remains in the user's "cloud." The user can then access his/her Dropbox account from a desktop computer and download the photograph to that computer.

31. Another feature of Dropbox is sharing. A Dropbox user can share certain files he/she designates by sending a web link to another user(s). It then gives the additional user(s) access to those particular files.

32. In general, a file that is saved to the subscriber's account at Dropbox, Inc., is stored in the subscriber's account on Dropbox, Inc. servers until the subscriber deletes the file. If the subscriber does not delete the file, the file can remain on Dropbox, Inc. servers indefinitely.

33. On-line storage providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, online storage providers often have records of the Internet Protocol address (IP address) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help identify which computers or other devices were used to access the account.

34. In some cases, Dropbox, Inc. account users will communicate directly with Dropbox, Inc. about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. On-line storage providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

35. Your Affiant knows that Dropbox maintains records on their users, such as basic subscriber information within the meaning of 18 U.S.C § 2703(c)(2). Furthermore, your Affiant knows that Dropbox keeps and maintains the stored content of user accounts, such as photographs, movies, documents and music within the meaning of the Stored Communication Act. Once the contents of the accounts are received, government investigators will review the records and copy those files that are specified in Attachment B. The investigation, as described more fully above, has revealed that the individual using the aforementioned email addresses did knowingly utilize

email to access, possess, transport or receive child pornography and that individual may be utilizing accounts at Dropbox, Inc., to store and share child pornography. There is probable cause to believe there is evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252(a)(2) and (a)(4)(B), are located at Dropbox, Inc., associated with the URLs listed in Attachment A and the following email accounts:

Woodsfamilyhome@gmail.com

Chris@ustechsolutions.com

cwoods@teksystems.com

bigmaninpa@gmail.com

bigmaninpa16@gmail.com

Chriswoods72@outlook.com

Chriswoods@synergy.com

Chris.woods@synergy.com

VI. Characteristics of Sex Offenders

36. Based on your Affiant's previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom your Affiant has had discussions, your Affiant has learned that individuals who view and receive multiple images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they

may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children almost always possess and maintain their “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain such materials for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer or mobile device or in online storage. These collections are often maintained for several years and are kept close by, usually at the collector’s residence, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may communicate with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such

communications as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. Those that receive and possess and collect child pornography maintain their collection and material even if they move physical, geographic locations. A collector and user of child pornography who maintains the images and videos in a digital or electronic format, such as in a cloud based or internet storage system, on a computer, discs, external hard drive, thumb drives, mobile devices, etc., will assure continued access to the materials and/or take the materials to a new location in the event of a physical move.

VII. Information to be Searched and Things to be Seized

37. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Dropbox, Inc., to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A. Upon receipt of the information described in Attachment A, government-authorized persons will review that information to locate the items described in Attachment B.

VIII. Conclusion

38. Based upon the information contained in this application and affidavit, there is probable cause to conclude that on the computer systems owned, maintained, and/or operated by

Dropbox.com there exists evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252(a)(2) and 2252(a)(4)(B) which makes it a crime to receive, distribute access or possess material depicting the sexual exploitation of a minor.

39. Your Affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search and seizure of the records and other information particularly described in Attachment A for the items listed and described in Attachment B.

40. Pursuant to Title 18, U.S.C. Section 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

41. Based on the Dropbox Law Enforcement Handbook, "Dropbox's policy is to provide notice to users about law enforcement requests for their information prior to complying with the request, unless prohibited by law. We might delay notice in cases involving the threat of death or bodily injury, or the exploitation of children." Your affiant respectfully requests this Court to issue an order to Dropbox, Inc., to not provide required notice to the subscriber or customer pursuant to Title 18, United States Code, Section 2703(b)(1)(A), and not to notify any person of the existence of this warrant for the next 180 days pursuant to Title 18, United States Code, Section 2705(b). This request is made because I believe notification of the existence of the warrant may result in the destruction or tampering with evidence and/or will seriously jeopardize the ongoing investigation. (Title 18, United States Code, Sections 2705(b)(3) and (5)).

42. Your Affiant respectfully requests that this Court issue an Order sealing, until further order of Court, all papers submitted in support of this Application, including the Application, Affidavit and attachments hereto, and the Search Warrant, and the requisite inventory notice (with the exception of one copy of the warrant and inventory notice that will be left at Dropbox, Inc., 185 Berry Street, 5th Floor, San Francisco, California 94107). Sealing is necessary

because the items and information to be seized are relevant to an ongoing investigation and premature disclosure of the contents of this Affidavit and related documents may have a negative impact on this continuing investigation and may jeopardize its effectiveness.

43. A separate motion for an order requiring non-disclosure of the search warrant to the subscriber pursuant to Title 18, United States Code, Section 2703(b)(1)(A), and Title 18, United States Code, Section 2705(b), is being filed simultaneously hereto.

44. The above information is true and correct to the best of my knowledge, information, and belief.

Respectfully submitted,



Thomas N. Carter
Special Agent
Federal Bureau of Investigations

Subscribed and sworn before me,
This 13th day of September, 2017.



CYNTHIA REED EDDY
United States Magistrate Judge